# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/912,390 | 07/26/2001 | Alexander James Hinchliffe | 550-249 | 5035 |

7590        12/22/2004

NIXON & VANDERHYE P.C.
8th Floor
1100 North Glebe Road
Arlington, VA 22201-4714

| EXAMINER |
|---|
| ZHEN, WEI Y |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2122 | |

DATE MAILED: 12/22/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

| | **Application No.** 09/912,390 | **Applicant(s)** HINCHLIFFE ET AL. |
|---|---|---|
| **Office Action Summary** | **Examiner** Wei Y Zhen | **Art Unit** 2122 | |

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1) ☒ Responsive to communication(s) filed on *17 August 2004*.

2a) ☒ This action is **FINAL**.      2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4) ☒ Claim(s) *1-39* is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) *1-39* is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☐ All   b)☐ Some * c)☐ None of:

   1.☐ Certified copies of the priority documents have been received.

   2.☐ Certified copies of the priority documents have been received in Application No. _____.

   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
   application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
   Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application (PTO-152)

6) ☐ Other: _____.

## DETAILED ACTION

1.      This office action is in response to the amendment filed 8/17/2004.

2.      Claims 1-39 are pending.


### *Claim Rejections - 35 USC § 102*

3.      The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999

(AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002

do not apply when the reference is a U.S. patent resulting directly or indirectly from an

international application filed before November 29, 2000. Therefore, the prior art date of the

reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA

35 U.S.C. 102(e)).

Claims 1-4, 6, 14-19, 27-32 are rejected under 35 U.S.C. 102(e) as being anticipated by

Diamant et al, U.S. Patent No. 6,202,153.

As per claim 1, Diamant et al. discloses

malware infection detecting logic operable to detect a malware infection of at least one

computer (col. 2 lines 4-7 and col. 13 lines 33-45)

device disabling logic operable upon diction of said malware infection to disable

operation of one or more data I/O devices of said at least one computer (col. 9 lines 48-54).

As per claim 2, Diamant et al. discloses

detects a malware infection by one or more of: positively identifying an item of malware

upon said at least one computer and identifying behavior of said at least one computer indicative

of malware infection (col. 2 lines 4-7, col. 9 lines 48-54 and col. 13 lines 33-45).

As per claim 3, Diamant et al disclose wherein one ore more data I/O devices include one

or more of: a flopping disk drive, a compact disk drive, a removable media drive and a network

interface card (Fig. 4, "I/O interface").

As per claim 4, Diamant et al discloses

wherein said device disabling logic is operable upon detection of malware infection to

disable at least one data I/O device of at least one further computer (col. 9 lines 48-54).

As per claim 6, Diamant et al discloses

said device disabling logic is operable to disable said one or more data I/O devices using

an API call to an operating system of said at least one computer (col. 9 lines 48-54 and Fig. 4).

Claims 14-19 are rejected for the reason set forth in the rejection of claims 1-6.

Claims 27-32 are rejected for the reason set forth in the rejection of claims 1-6.

### *Claim Rejections - 35 USC § 103*

4.      The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

Claims 7-9, 20-22, 33-35 are rejected under 35 U.S.C. 103(a) as being unpatentable over

Diamant et al, U.S. Patent No. 6,202,153.

Claims 7-9 are rejected for the reason set forth in the rejection of claims 1, 3, 6.

As per claim 7, Diamant et al disclose device disabling logic operable upon receipt by a

computer of a command indicative of malware infection precautions being taken to disable

operation of one or more data I/O devices of said computer (see rejection to claim 1 above).

Diamant does not explicitly disclose receipt by a first computer of a command generated by a

second computer as claimed. However, official notice is taken that exchanging instructions

between computers to remotely control executions of computer was well know in the art at the

time the invention was made. Therefore, it would have been obvious to one having ordinary skill

in the art to incorporate the teaching of the well known knowledge into the teaching of Diamant

et al to have receipt by a first computer of a command generated by a second computer as

claimed because one would want to be able to remotely control the operation of computers.

As per claim 8, the rejections of claim 7 is incorporated and further it is rejected as the

reason set forth in the rejection of claim 3.

As per claim 9, the rejections of claim 7 is incorporated and further it is rejected as the reason set forth in the rejection of claim 6.

Claims 20-22 are rejected for the reason set forth in the rejection of claims 7-9.

Claims 33-35 are rejected for the reason set forth in the rejection of claims 7-9.


5.      Claims 5, 10-13, 23-26, 36-39 are rejected under 35 U.S.C. 103(a) as being unpatentable over Diamant et al, U.S. Patent No. 6,202,153 in view of Reardon, U.S. Patent No. 6,212,635.

As per claim 5, the rejection of claim 1 is incorporated and further Diamant et al does not explicitly disclose wherein said device disabling logic is operable to require user confirmation prior to disabling said one or more data I/O devices.

However,  Reardon discloses require user confirmation prior to disabling data I/O devices (col. 29 lines 25-50).

Therefore, it would have been obvious to one having ordinary skill in the art to incorporate the teaching of Reardon into the teaching of Diamant et al to have the device disabling logic is operable to require user confirmation prior to disabling said one or more data I/O devices.  The modification would have been obvious because one would want to have the user to have the flexibility to choose the action one would want to take against the malware infection.

As per claim 10, the combinations of Diamant et al and Reardon disclose the claimed the limitations (see rejections of claim 1 and 5 above) except the combination of Diamant and Reardon does not explicitly disclose receipt by a first computer of a command generated by a second computer to instruct operation of computer as claimed. However, official notice is taken

that exchanging instructions between computers to remotely control executions of computer was

well know in the art at the time the invention was made. Therefore, it would have been obvious

to one having ordinary skill in the art to incorporate the teaching of the well known knowledge

into the teaching of Diamant et al to have receipt by a first computer of a command generated by

a second computer to instruct the operations of computers as claimed because one would want to

be able to remotely control the operation of computers.

As per claims 11-13, the rejection of claim 10 is incorporated and further claims 11-13

are rejected for the reason set forth in the rejections of claims 3, 4, 6.

Claim 23 is rejected for the reason set forth in the rejection of claim 10.

As per claim 24-26, the rejection of claim 23 is incorporated and further claims 24-26 are

rejected for the reason set forth in the rejections of claims 3, 4, 6.

Claim 36 is rejected for the reason set forth in the rejection of claim 10.

As per claims 37-39, the rejections of claim 36 is incorporated and further claims 37-39

are rejected for the reason set forth in the rejections of claims 3, 4, 6.

### Response to Arguments

6.     Applicant's arguments with regard to claims 1, 14 and 27 have been fully considered but

they are not persuasive.

Applicant has argued:

a)     Diamant does not disclose detect that a malware infection has occurred in at least one

computer and any mechanism and "device disabling logic that is operable upon detection of said

malware infection".

Examiner's response:

a)      Examiner disagrees with applicant's assertion that Diamant does not disclose the above

mentioned limitation. Diamant disclose this limitation at col. 9 lines 40-52. Note that the

examiner is interpreting the malware infected computer as a computer that another computer/user

is denied access to. Diamant clearly disclose device disabling logic that is operable upon the

detection of the malware infected computer (a secured terminal is being accessed by a non-

secured terminal) at col. 9 lines 40-52.

7.      Applicant's arguments with respect to claims 7-13, 20-26, 33-39 have been considered

but are moot in view of the new ground(s) of rejection.


### *Conclusion*

8.      Applicant's amendment necessitated the new ground(s) of rejection presented in this

Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a).

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within TWO

MONTHS of the mailing date of this final action and the advisory action is not mailed until after

the end of the THREE-MONTH shortened statutory period, then the shortened statutory period

will expire on the date the advisory action is mailed, and any extension fee pursuant to 37

CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this

final action.

9.      Any inquiry concerning this communication or earlier communications from the

examiner should be directed to Wei Y Zhen whose telephone number is (571) 272-3708. The

examiner can normally be reached on Monday-Friday, 8 a.m. - 4:30 p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's

supervisor, Tuan Dam can be reached on (571) 272-3695. The fax phone number for the

organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent

Application Information Retrieval (PAIR) system.  Status information for published applications

may be obtained from either Private PAIR or Public PAIR.  Status information for unpublished

applications is available through Private PAIR only.  For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR

system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Wei Zhen
12/16/2004

**WEI Y. ZHEN**
**PRIMARY EXAMINER**